

ОГЛАВЛЕНИЕ

Предисловие	3
Введение	7
1. Нормативная база управления инцидентами ИБ и обеспечение непрерывности бизнеса	9
1.1. ISO/IEC 27035:2011 – управление инцидентами ИБ	10
1.2. ISO/IEC 27037 – руководство по идентификации, сбору и/или получению и обеспечению сохранности свидетельств, представленных в электронной форме	12
1.3. ISO/IEC 27031:2011 – руководство по готовности информационных и телекоммуникационных технологий для обеспечения непрерывности бизнеса	14
1.4. BS 25999 и ГОСТ Р 53647 – управление непрерывностью бизнеса	17
Выводы	18
Вопросы для самоконтроля	19
2. Управление инцидентами ИБ	20
2.1. Событие и инцидент ИБ	21
2.2. Цели и задачи управления инцидентами ИБ	26
2.3. Система управления инцидентами ИБ	31
2.4. Этапы процесса управления инцидентами ИБ	39
2.4.1. Планирование и подготовка процесса управления инцидентами ИБ	40
2.4.2. Использование системы управления инцидентами ИБ	41
2.4.3. Анализ процесса управления инцидентами ИБ	43
2.4.4. Улучшение процесса управления инцидентами ИБ	45
2.5. Обнаружение событий ИБ и инцидентов ИБ и оповещение о них	46
2.6. Обработка событий ИБ и инцидентов ИБ	48
2.6.1. Первая оценка и предварительное решение по событию ИБ	49
2.6.2. Вторая оценка и подтверждение инцидента ИБ	53
2.7. Реагирование на инциденты ИБ	55
2.7.1. Немедленное реагирование на инцидент ИБ	56
2.7.2. Контролируемость инцидента ИБ	59
2.7.3. Последующее реагирование на инцидент ИБ	59
2.7.4. Антикризисные действия	60
2.7.5. Правовая экспертиза инцидентов ИБ	61
2.7.6. Передача информации	66
2.7.7. Расширение области принятия решений	67

2.7.8. Регистрация деятельности и контроль за внесением изменений	67
2.7.9. Техническая поддержка реагирования на инциденты ИБ	67
2.8. Документация системы управления инцидентами ИБ	69
2.8.1. Политика управления инцидентами ИБ	71
2.8.2. Программа управления инцидентами ИБ	72
2.9. Группа реагирования на инциденты ИБ	77
2.10. Обеспечение осведомленности и обучение в области инцидентов ИБ	83
2.11. Сохранение доказательств инцидента ИБ	84
2.12. Средства управления событиями ИБ	90
Выводы	92
Вопросы для самоконтроля	93
3. Управление непрерывностью бизнеса организации	96
3.1. Определения непрерывности бизнеса и управления ею	99
3.2. Система управления непрерывностью бизнеса	103
3.3. Жизненный цикл управления непрерывностью бизнеса	105
3.3.1. Управление программой УНБ	107
3.3.2. Анализ непрерывности бизнеса организации	110
3.3.3. Определение стратегии УНБ	116
3.3.4. Разработка и внедрение в УНБ ответных мер на инциденты	121
3.3.5. Меры по применению, поддержке и анализу УНБ	125
3.3.6. Внедрение УНБ в культуру организации	134
3.4. Документация и записи в области непрерывности бизнеса	136
3.4.1. Политика УНБ	137
3.4.2. Планы управления инцидентом, ОНБ и восстановления бизнеса	139
3.5. Готовность ИТТ к ОНБ	151
3.6. Средства управления непрерывностью бизнеса	157
Выводы	158
Вопросы для самоконтроля	158
Заключение	160
Приложения	163
Примеры систем управления событиями ИБ	163
Принятые сокращения	163
Список литературы	165